

# Shortest Distance in Modular Cubic Polynomials

Tsz Ho Chan

## Abstract

In this paper, we study how small a box contains at least two points from a modular cubic polynomial  $y \equiv ax^3 + bx^2 + cx + d \pmod{p}$  with  $(a, p) = 1$ . We prove that some square of side length  $p^{1/6+\epsilon}$  contains two such points.

## 1 Introduction and Main results

Recently, the author [1] studied the shortest distance in modular hyperbola  $xy \equiv c \pmod{p}$  and its relation with the least quadratic nonresidue modulo  $p$ . Inspired by this, we study the shortest distance in modular cubic polynomial in this paper. It is worthwhile to remark that, the shortest distance can have magnitude  $p$  for linear polynomials while the shortest distance can be as small as  $O(1)$  for quadratic polynomials.

Let  $p > 3$  be a prime,  $(a, p) = 1$  and any integer  $c$ . We consider the modular reduced cubic

$$C_{a,c} := \{(x, y) : y \equiv ax^3 + cx \pmod{p}\}.$$

The restriction to such reduced cubic polynomials is not restrictive at all as one can transform a general cubic to such form through change of variables in  $x$  and  $y$  which does not affect the shortest distance between two points in  $C_{a,c}$ . Instead of distances, we consider how small a box

$$B(X, Y; H) := \{(x, y) : X + 1 \leq x \leq X + H \pmod{p}, Y + 1 \leq y \leq Y + H \pmod{p}\}$$

contains at least two points in  $C_{a,c}$  where  $X$  and  $Y$  run over  $0, 1, \dots, p-1$ .

To study this, we use a recent result of Heath-Brown [2] and Shao [3] on mean-value estimates of character sums:

**Theorem 1** *Given  $H \leq p$ , a positive integer and any  $\epsilon > 0$ . Suppose that  $0 \leq N_1 < N_2 < \dots < N_J < p$  are integers satisfying  $N_{j+1} - N_j \geq H$  for  $1 \leq j < J$ . Then*

$$\sum_{j=1}^J \max_{h \leq H} |S(N_j; h)|^{2r} \ll_{\epsilon, r} H^{2r-2} p^{1/2+1/(2r)+\epsilon}$$

where

$$S(N; H) := \sum_{N < n \leq N+H} \chi(n)$$

and  $\chi$  is any non-principal character modulo  $p$ .

Applying the above theorem, we can show that

**Theorem 2** *For any  $\epsilon > 0$ , for any  $(a, p) = 1$ , integer  $c$  and  $H \gg_{\epsilon} p^{1/6+\epsilon}$ , we have*

$$|C_{a,c} \cap B(X, Y; H)| \geq 2$$

for some  $0 \leq X, Y \leq p-1$ .

**Some Notations** Throughout the paper,  $p$  stands for a prime. The symbol  $|S|$  denotes the number of elements in the set  $S$ . We also use the Legendre symbol  $(\frac{\cdot}{p})$ . The notations  $f(x) \ll g(x)$ ,  $g(x) \gg f(x)$  and  $f(x) = O(g(x))$  are equivalent to  $|f(x)| \leq Cg(x)$  for some constant  $C > 0$ . Finally,  $f(x) \ll_{\lambda_1, \dots, \lambda_k} g(x)$ ,  $g(x) \gg_{\lambda_1, \dots, \lambda_k} f(x)$  and  $f(x) = O_{\lambda_1, \dots, \lambda_k}(g(x))$  mean that the implicit constant  $C$  may depend on  $\lambda_1, \dots, \lambda_k$ .

## 2 The Basic Argument

Without loss of generality, we assume that  $p > 3$ . For  $(a, p) = 1$  and any integer  $c$ , suppose  $|C_{a,c} \cap B(X, Y; H)| \geq 2$  for some  $0 \leq X, Y \leq p-1$ . This means that

$$y \equiv ax^3 + cx \pmod{p}, \text{ and } y + v \equiv a(x + u)^3 + c(x + u) \pmod{p} \quad (1)$$

for some  $1 \leq x, y \leq p$  and  $1 \leq u, v \leq H$ . Subtracting, we get

$$v \equiv 3au(x^2 + ux + \overline{3}u^2) + cu \pmod{p}$$

where  $\overline{y}$  denotes the multiplicative inverse of  $y$  modulo  $p$  (i.e.  $y\overline{y} \equiv 1 \pmod{p}$ .) After some algebra and completing the square, we have

$$(2x + u)^2 \equiv 4\overline{3}v\overline{au} - \overline{3}u^2 - 4\overline{3}\overline{ac} \pmod{p}.$$

The above process is reversible. So  $|C_{a,c} \cap B(X, Y; H)| \geq 2$  for some  $0 \leq X, Y \leq p-1$  is equivalent to

$$\left(\frac{-3}{p}\right)\left(\frac{a}{p}\right)\left(\frac{u}{p}\right)\left(\frac{au^3 + 4cu - 4v}{p}\right) = 1.$$

We are going to restrict our attention to even  $u = 2u'$ 's and  $v = 2v'$ 's. So we want

$$\left(\frac{-3}{p}\right)\left(\frac{a}{p}\right)\left(\frac{u'}{p}\right)\left(\frac{au'^3 + cu' - v'}{p}\right) = 1 \text{ for some } 1 \leq u', v' \leq H/2. \quad (2)$$

## 3 Proof of Theorem 2

Suppose (2) is not true. Then either

$$\left(\frac{-3}{p}\right)\left(\frac{a}{p}\right)\left(\frac{u'}{p}\right)\left(\frac{au'^3 + cu' - v'}{p}\right) = 0;$$

or

$$\left(\frac{-3}{p}\right)\left(\frac{a}{p}\right)\left(\frac{u'}{p}\right)\left(\frac{au'^3 + cu' - v'}{p}\right) = -1$$

for all  $1 \leq u', v' \leq H/2$ . If the former is true for two pairs of  $1 \leq u', v' \leq H/2$ , we have

$$au'^3 + cu' \equiv v' \pmod{p} \text{ and } au''^3 + cu'' \equiv v'' \pmod{p} \quad (3)$$

which gives Theorem 2. Henceforth we suppose the latter is true for all but at most one pair of  $1 \leq u', v' \leq H/2$ . Hence

$$\begin{aligned} H^2 &\ll \left| \sum_{u' \leq H/2} \sum_{v' \leq H/2} \left(\frac{u'}{p}\right) \left(\frac{au'^3 + cu' - v'}{p}\right) \right| \leq \sum_{u' \leq H/2} \left| \sum_{v' \leq H/2} \left(\frac{au'^3 + cu' - v'}{p}\right) \right| \\ &\leq \left( \sum_{u' \leq H/2} 1 \right)^{(2r-1)/(2r)} \left( \sum_{u' \leq H/2} \left| \sum_{v' \leq H/2} \left(\frac{au'^3 + cu' - v'}{p}\right) \right|^{2r} \right)^{1/(2r)}. \end{aligned}$$

Suppose  $|C_{a,c} \cap B(X, Y; H)| \leq 1$  for all  $0 \leq X, Y \leq p-1$ . Then the points  $au'^3 + cu'$  are spaced more than  $H$  apart. So we can apply Theorem 1 and get

$$H^2 \ll_{\epsilon, r} H^{(2r-1)/(2r)} (H^{2r-2} p^{1/2+1/(2r)+\epsilon})^{1/(2r)}$$

which gives  $H \ll_{\epsilon, r} p^{(r+1)/(6r)+\epsilon/2}$ . This contradicts  $H \gg_{\epsilon} p^{1/6+\epsilon}$  if  $r$  is sufficiently large. This final contradiction together with (3) gives Theorem 2.

## References

- [1] T.H. Chan, *Shortest Distance in Modular Hyperbola and Least Quadratic Nonresidue*, submitted.
- [2] D.R. Heath-Brown, *Burgess's bounds for character sums*, Number theory and related fields, 199-213, Springer Proc. Math. Stat., 43, Springer, New York, 2013.
- [3] X. Shao, *Character Sums over Unions of Intervals*, ArXiv e-prints, [arxiv.org/pdf/1302.0348](https://arxiv.org/pdf/1302.0348).

Tsz Ho Chan  
 Department of Mathematical Sciences  
 University of Memphis  
 Memphis, TN 38152  
 U.S.A.  
[thchan6174@gmail.com](mailto:thchan6174@gmail.com)